

Amendments to the Claims

Please amend Claims 1, 7, 12 and 18. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. (Currently Amended) An agent process for controlling access to digital assets in a ~~data processing environment~~ network of data processing devices comprising:

defining a security perimeter that includes two or more data processing devices;

defining one or more policy violation predicates, to be asserted when a possible risk of use of a digital asset by an end user outside of the security perimeter occurs;

sensing atomic level digital asset access events, the sensing step located within an operating system kernel within [[a]] an end user client device, at a point of authorized access to the digital asset by the end user;

aggregating multiple atomic level events to determine a combined event; and

asserting a policy violation predicate if [[a]] at least one combined event has occurred that violates a predefined digital asset usage policy that indicates a risk of use of the digital asset outside of the security perimeter.

2. (Original) A process as in Claim 1 wherein the step of asserting the policy violation predicate is implemented in an operating system kernel of the client user device.

3. (Original) A process as in Claim 1 additionally comprising:

preventing a user from accessing the digital asset if the policy predicate indicates a violated policy.

4. (Original) A process as in Claim 3 wherein the preventing step includes an IRP intercept.
5. (Original) A process as in Claim 1 wherein the combined event is a time sequence of multiple atomic level events.
6. (Original) A process as in Claim 1 additionally comprising:
prompting a user to document a reason for a policy violation, prior to granting access to the digital asset.
7. (Currently Amended) A process as in Claim 1 additionally comprising:
~~asserting multiple policy violation predicates such that any one predicate can veto the operation of other predicates. prior to indicating a risk of use of the digital asset outside of the security perimeter.~~
8. (Original) A process as in Claim 2 that operates independently of application software.
9. (Original) A process as in Claim 1 additionally comprising:
notifying a user of a policy violation, and then permitting access to the digital asset.
10. (Original) A process as in Claim 2 wherein the sensors, aggregators, and asserting steps operate in real time.
11. (Original) A process as in Claim 1 additionally comprising:
determining the identity of a particular file in the asset access event.
12. (Currently Amended) A system for controlling access to digital assets in a ~~data processing environment~~ network of data processing devices comprising:

a digital asset usage policy server, for storing one or more digital asset usage policies to be applied to a security perimeter, the security perimeter comprising two or more data processing devices;

an atomic level data processing asset access event sensor, the sensor located within an operating system kernel within [[a]] an end user client device, to sense atomic level events at a point of authorized access by the end user device to one or more digital assets;

an atomic level event aggregator, to determine the occurrence of an aggregate event that comprises more than one atomic level asset access event; and

a policy violation detector, for determining if a combination of combined events have occurred that violates a predefined digital asset usage policy that indicates a risk of use of a digital asset outside the security perimeter.

13. (Original) An apparatus as in Claim 12 wherein the policy violation detector is located in an operating system kernel of the user client device.

14. (Original) An apparatus as in Claim 12 wherein the policy violation detector determines a violated policy type.

15. (Original) An apparatus as in Claim 14 wherein the policy violation detector includes an IRP intercept.

16. (Original) An apparatus as in Claim 12 wherein the combined event is a time sequence of multiple atomic level events.

17. (Original) An apparatus as in Claim 12 wherein a user interface within the client device requires a user to document a reason for a policy violation prior to granting access to the digital asset.

18. (Currently Amended) As apparatus as in Claim 12 wherein the policy violation detector additionally asserts multiple policy violation predicates such that any one predicate can veto the

operation of other predicates prior to indicating a risk of use of the digital asset outside of the security perimeter.

19. (Original) An apparatus as in Claim 13 that operates independently of application software.
20. (Original) An apparatus as in Claim 12 additionally comprising:
a user interface running on the user client device for notifying a user of a policy violation;
and
permitting access to the digital asset once a reason for the violation is provided by the user.
21. (Original) An apparatus as in Claim 12 wherein the sensor, aggregator and detector operate in real time.
22. (Original) An apparatus as in Claim 12 wherein the detector additionally determines the identity of a particular file in the atomic level asset event.